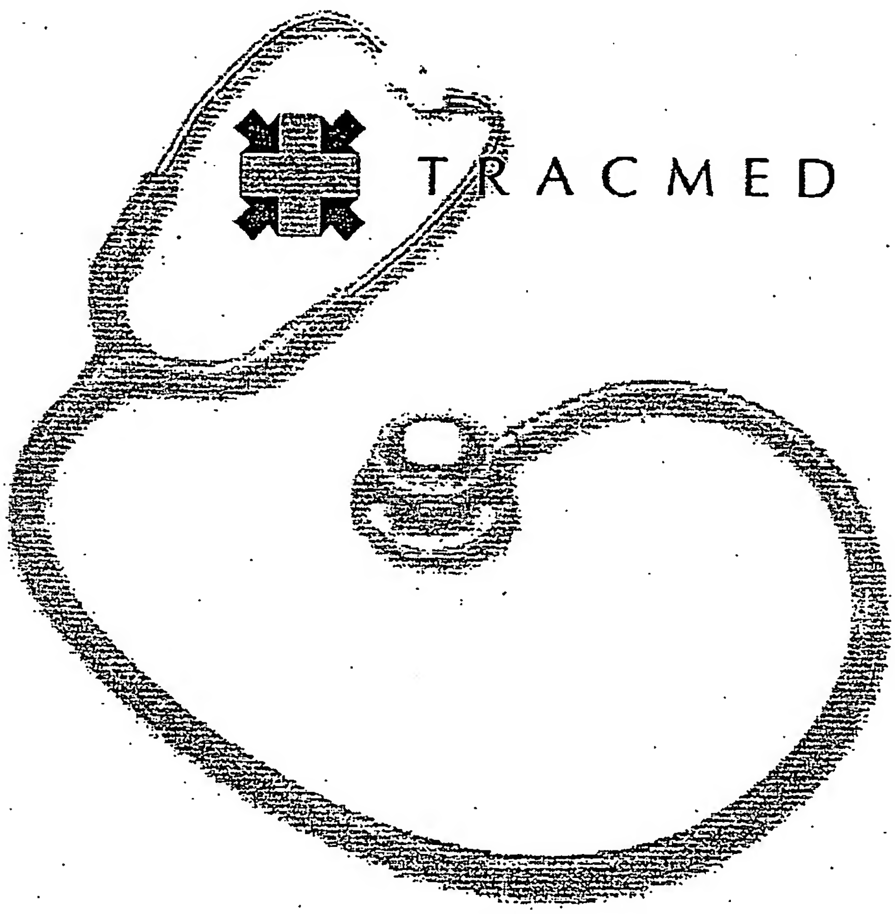
APPENDIX

Building a Common-Sense Home Healthcare Secure Internet Strategy



TRAC Medical, Inc.
5711 Six Forks Road, Suite 308
Raleigh, NC
(919) 676-6625
www.tracmed.c m

A1:

EXECUTIVE SUMMARY

Trac Medical seeks to deliver a secure healthcare transaction network and application platform that embraces requirements for certification of use for durable medical equipment in the home health marketplace. The *e*CareXchange system provides a secure and expeditious means for durable medical equipment (DME) providers to get the necessary authorization from physicians to place medical devices for their patients in a homecare setting. Our model calls for a revenue based on each certification that is processed through our secure portal. Present paper based system involves a labor intensive process that extends accounts receivable and directly impacts business work flow process of the DME and physician.

The healthcare industry faces a growing number of challenges with respect to regulations surrounding the confidentiality, integrity, and availability of individual health information. This increasingly complex regulatory environment received added momentum on August 12, 1998, with the Notice of Proposed Rule from the Department of Health and Human Services. The Proposed Rule falls under the umbrella of the Health Insurance Portability and Accountability Act, perhaps better known as the Kennedy Kassebaum Bill and this Bill was passed on August 21, 1996. HIPAA contained a sectioned entitled, "Administrative Simplification" and the Health Care Financing Administration (HCFA) is responsible for implementing the Administrative Simplification. Recently (August 12th, 1998) the HCFA and the Department of Health and Human Services released a Notice of Proposed Rule Security and Electronic Signature Standards (45 CFR, Part 142). This Proposed Rule suggests standards for the security of individual health information and electronic signature for use by health plans, health care clearinghouses, and health care providers. The health plans, health care clearinghouses, and health care providers would use the security standards to develop and maintain the security of all electronic health information. The recent Proposed Rule is not to be confused with Privacy legislation, which attempts to establish privilege rights for individual health information. The proposed Security and Electronic Signature standard establishes the technical measures that guard against inappropriate access and use. The final rules and standards are to be published in the 4th quarter of 2000.

In today's home care industry compliance and fiscal management are keynotes for survival. Increased scrutiny by fiscal intermediaries, managed care entities and federal auditors are mandating preemptive measures for accountability. According to the Office of Inspector General for Health and Human Services, eligibility is the number one priority for scrutiny in home health care. It seems safe to assume that most physicians and durable medical equipment suppliers are aware of the need to institute compliance programs as a safeguard against possible prosecution and penalties. The ability to verify with a high degree of certainty the integrity of medical necessity is paramount in avoiding issues of liability. The capacity to increase cash flow through the expediency of claims processing is critical to fiscal management. The following issues of compliance are addressed by this technology platform.

- Document Integrity
- Non-repudiation of User Identity
- Host Data Base Independent

- Integral Time and Date Stamp
- User Authentication
- Independent Verification
- Third Party Audit

The durable medical equipment industry is $8 billion industry represented by more than 1200 equipment providers nationwide. The majority of these providers are members of the American Association of Homecare located in Alexandria, Virginia. This trade organization has assigned a **first priority status** to assist Trac Medical in implementation of our technology base in regards to regulatory approvals and implementation to their trade membership.

The TracMed *e*CareXchange is a business management and regulatory compliance tool for home health medical device providers. Initial responses have indicated that significant saving in physician and provider manpower hours may be realized in productivity and streamlining of billing process. It meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by documenting agency and provider activities as it relates to eligibility and medical necessity so as to reduce fraud and abuse.

The TracMed *e*CareXchange system entails the use of a secure Web server that assures confidentiality and integrity of patient records sent between home health provider and physician. The secure web page is designed with firewall and encryption/decryption capability for presentation of Certificate for Medical Necessity to appropriate patient's physician or referring home health agency. Upon assessment that the patient is in need of a medical device a request for certification is transmitted to patient's physician via e-mail system. Interface with the Home Health Agency may be required for proper clinical information to be included within documentation presented to the physician. The design of the system allows presentation to all parties (DME, HHA and physician) involved in the certification process. This allows the certification process to originate from within any one of these entities with the ultimate signatory process residing with patient's physician. Certification of medical necessity is determined by prescribing physician in accordance with HCFA standards based on treatment records and patient condition by linking to secure web site and logging into patient database using secure pass codes. Electronic signature is accomplished by digital certificate issued from an approved authenticating authority. The signature is embedded within the document and encryption of the entire document format eliminates alterations after signature. Database may be audited electronically by a third party intermediary for integrity and authenticity therefore assuring medical necessity forms have not be altered or augmented without the explicit consent of the prescribing physician. Treatment review (re-certification and change orders) may be updated via the electronic format as need indicates. Claims processing become a much speedier and efficient task resulting in dramatic increases in cash flow. Issues of document integrity and confidentiality are greatly diminished due to encrypted database and secure web site with the ability for fiscal intermediary to overview electronically. Cost per document processing is greatly reduced and encrypted format exceeds integrity standards of paper-based system.

Business Profile

There are two industry segments of interest in analyzing this business. The customers are primarily part of the Home Health Care Services segment (SIC 8082). Trac Medical is primarily a software integration firm in the Computer Integrated Systems Design segment (SIC 7373)

Core Technology

Our core competency resides in an extensible web object technology (XML based) for dealing with health care form processing on a secure PKI web server. We utilize a template object populated via a dynamic (replacement) database with the ability to affix a digital signature resulting in a bundled web object in an XML format. XML form may be manipulated by or presented to authorized or credentialed users. We consider this core technology to be in the very forefront of development initiatives in this area.

Current Size

There were 1238 durable medical equipment providers and 9,027 Medicare-certified home health agencies as of December 1999. These agencies and providers serviced 3.735 million patients with 285 million visits from 666 thousand full time employees. (Source: National Association for Home Care 1999 Home Care Statistics)

Technology Solution

The Tracmed.com solution is a private, secure, Internet-based transaction network for the use of physicians and providers in the home healthcare industry. The solution will be an application service provider platform with a PKI secure server.

Industry Trends

Continued interest in reducing deficits and control work processes will continue to apply pressure to DMEs to reduce costs and fight fraud and abuse. There is a trend, therefore, toward implementation of technology to supplement or replace existing paper based systems.

PRODUCT TECHNOLOGY DEVELOPMENT

The Trac Medical system has two essential components

- Certificate of Medical Necessity Verification for equipment placement
- Electronic Audit by third party

Pilot Project

A pilot will demonstrate:

- The ability to digitally authenticate and signature CMNs on a secure web server
- The overall savings in processing time from CMN creation to Medicare billing.
- The physician acceptance of an Internet solution.
- The eCMN requires that physicians and suppliers have Internet access.

Descriptive:

Implement a pilot program consisting of a defined 100-physician test base group benchmarked against a defined 100-physician control group. The MEDePASS Corporation will administer physician and provider credentialing under the guidelines of the PKI server standards defined by HCFA. Geographical location of pilot will be Raleigh-Durham, North Carolina area. Supplier participants would participate from respective regional centers within the test area. Carrier participant will be Palmetto GBA Region C that is intermediary for Medicare reimbursement in 26 states.

Initiatives

Introduce electronic signature and transmission of certificate for medical necessity documentation utilizing digital certificates and a secure web server.

Platform Architecture

- Electronic Signature utilizing digital certificates from MEDePASS, Inc.
- Authentication utilizing notary public verification of identity
- SSL 3.0 Secure Sockets Layer (SSL) (Sometimes referred to as Transport Layer Security - TLS) implementations - At a minimum SSL level of Version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets Layer. 128/1024 Encryption
- HCFA/OMB Document in XML format

Feature Set of Platform

- Inactive File Archiving and Retrieval
- Encrypted Format (Document Integrity)
- Integral Assisted ICD-9 Coding Tables
- Secure Web Server (Patient Confidentiality)
- Signature Forensics Through Shared Secrets (User Authentication)
- Client Data Base Independent (Server Repository of Data and Digital Certificates)
- Web Based Chronometer (Time and Date Stamp)
- Fiscal Intermediary Access (Third Party Audit)
- The major components of system include:
- eCMN database
- Physician database
- Supplier database
- Internet accessibility to eCMN forms.
- Digital Certification
- Reports

A description of each component is given below followed by usage scenarios.

eCMN database

This database contains the eCMN documents that have been signed as well as those that are in the process of being created. The digitally signed documents must be retained in the database at least 5 years from the date that the bill for the equipment is sent to DMERC (Durable Medical Equipment Regional Carrier). There are 63 million claims per year submitted. Apria and Hill-Rom combine for over 11.2 million claims.

Physician database

This database contains the physicians who have obtained a digital id and are authorized to initiate and complete eCMN's. There is at least enough information contained in the database about each physician to fill in section A of an eCMN and to properly authenticate that physician.

Supplier database

This database contains the information about the suppliers or home health agencies. Since the suppliers are responsible for signing immunosuppressive drug forms, they must also receive a digital ID. Enough information about each supplier must be maintained to allow automatically filling in section A as well as to properly authenticating him or her.

Internet accessibility to eCMN forms

The forms must be viewable over the Internet via a secure channel (SSL – secure sockets layer) to prevent unauthorized access.

The process for managing the forms and notifying the physician and supplier of required activities is also supported over the Internet. This process must be well organized allowing easy access to the forms to be created, reviewed, signed, or audited. Certain sections of the form must be restricted as to who can complete them. Section B of the CMN is to be filled out only by the physician or his agent. The supplier may only fill in section C. The physician may only fill in section D himself.

Notification via e-mail is accomplished by allowing each process state transition of the document to trigger an event. For example, when the supplier completes section B, the physician listed in section A is notified via e-mail. In addition, we should provide nag notes, email updates sent to the user after a certain time has elapsed without any action. Since physicians work round the clock, access to the eCMN forms should be available 24 hours a day 7 days a week. This will allow physicians off-hour opportunities to process this type of paperwork. Some down time for maintenance and backups is allowable during off-hours.

Digital Certification

In order to support a digital signature a trusted certification authority must be established to maintain a public key infrastructure. The certification authority is responsible for:

- Issuing a private key, which the physician can use to digitally, sign the eCMN.
- Maintaining the public key for verifying the signature and the integrity of the signed eCMN.
- Updating the private and public keys on a regular basis (annually) to ensure that the
- In order to be usable by the physicians, the electronic signature process must not take more time than it currently takes to physically sign a document.

Reports

The product must be able to generate reports based on the information contained within the CMN database. Reports should be broken down by:

- Patient
- Physician
- Supplier

Dates the reports need to cover:

- The elapsed time between process steps, for example DME request and Physician approval.
- % rejects
- % non-billable visits

Physician *Usage Scenarios*

Create and send eCMN to Supplier

The physician creates the eCMN filling out sections A and B then sends the document to the supplier to fill out section C. Note that a revised eCMN may be generated from an existing eCMN if the patient's level of care changes or if the patient is re-certified. In this case, sections A, B, and C of the new form should be filled in automatically from the previous version of the form and the forms should be linked together in the database.

Once an eCMN is signed all changes to the document will be versioned and the initial and revised date fields will be automatically filled in..

Approve Completed eCMN

After sections A, B, and C are filled out the physician must be notified. He must then review the form and sign it. Once approved, the agency (if any) and supplier are notified. A hardcopy of the form may be printed out and placed in the patients' medical records.

Obtain Digital Certificate

The physician fills out our request for digital certificate (signature card) and sends it to the certification authority. The card needs to include enough demographics about the physician to distinguish him. Namely, name, email, address, UPIN, phone... Certification authority then sends the physician an e-mail directing him to register. The MEDePASS certification model will be implemented (See Issuing MEDePASS Certifications).

DMERC Usage Scenarios

Audit eCMN for a patient

The pilot needs to determine the requirements for auditing eCMNs, such as whether or not we allow summary views of all eCMNs for a physician, for an agency, or for a supplier. The supplier will help flesh out the requirements since the supplier is the entity that must support the audit.

Supplier Usage Scenarios

Request physician authorization for patient equipment

Completes section C (and maybe A) and sends it to the physician for signature. In some cases (e.g. a revised eCMN) section C will be filled out. The supplier still needs to indicate that it approved the information listed in section C.

Integration Requirements Usage Scenario

Clinical System

Importing the patient/physician/supplier information (depends on how much of the information the system contains) from the clinical system to create the initial form would be a delighter. We should provide an API to allow a clinical system to export the information to us.

Billing System

It would be a delighter to trigger the supplier's billing system to send the bill to Medicare once the physician has signed the eCMN. If we pursue the execution of this project we must determine what billing systems the suppliers are using.

Trac Medical must automatically bill the supplier for use of the system.

Additional Requirements

In addition to the requirements stated above, eCMN must meet the following system infrastructure requirements:

- The system infrastructure will provide guaranteed qualities of service (QoS) such as uptime, response time, computation time, transaction integrity, etc.
- This provision will ensure no customer dissatisfaction due to technical problems, and will enable the sales staff to write these terms into contracts if necessary.
- The system infrastructure will provide access to a wide range of programming languages, operating systems, and, to some extent, network protocols.
- This provision will ensure system infrastructure flexibility in order to meet changing client demands, and will minimize development and testing costs associated with learning new technologies.
- The system infrastructure will provide access in a manner that is relatively consistent among the various programming languages, operating systems, and network protocols.

- This provision will enable application integration. It will also decrease development and testing time due to a consistent method of system access from dissimilar clients.
- The system infrastructure will provide centralized administration, monitoring, and maintenance capabilities for some modules that are at customer facilities.
- This provision will increase customer satisfaction by enabling remote troubleshooting of some parts of the system. It will also reduce the total cost of technical support.
- The system infrastructure will provide protection for customer data considered essential to each customer's success.

This provision will decrease possible liability issues for TRAC Medical and increase customer satisfaction. It is vital that suppliers not be able to view each other's information, either on-line or via reports.

- The system infrastructure should be as modular as it is beneficial. This provision will provide flexibility for future design changes, and enable rigorous testing processes.
- The system infrastructure will allow a staged development and deployment schedule.

This provision will allow basic functionality to be delivered in early stages without requiring substantial code re-writes for later stages.

Performance Metrics

1. Time of cycle for electronic versus paper based system
2. Cost of processing electronic version versus paper based system for all entities
3. Claims denial rate comparative test group/control group
4. Physician compliance and acceptance
5. Supplier compliance and acceptance

Goals

Supplier

- Increase cash flow by shortening billing cycle time
- Increase compliance initiatives
- Qualified physician database
- Better physician interface and communication
- Decrease clerical processing time
- Better clinical treatment
- Decrease denial rates due to improper form preparation

Physician

- 100% assurance of CMN integrity
- Integral ICD-9 coding data set
- Better knowledge and control of patient treatment
- Decrease administrative time

Carrier

- 100% overview of eligibility status
- Offsite audit capability
- Decrease cost for administration
- Meet or exceed HCFA compliance initiatives for eligibility

Patient

- Timely establishment of eligibility
- Defined treatment regimens
- Better patient/physician communication
- Avoid issues of unexpected payment responsibility

SUPPORTING DOCUMENTATION

Homecare Fraud and Abuse Issues

In a recent published article Secretary of Health and Human Services Donna Shalala stated, "that 25 to 40 percent of home health visits paid for by Medicare were for services that were either never delivered or were provided to people who did not qualify for their services".

Efforts by the federal government at this juncture to validate and verify eligibility for home care and the need for a medical device has been basically flawed.

The Importance of Physician Certification of Home Health Services

The Medicare program only pays for health care services that are medically necessary. In determining what services are medically necessary, Medicare primarily relies on the professional judgment of the beneficiary's treating physician, since he or she knows the patient's history and makes critical decisions, such as admitting the patient to the hospital; ordering tests, drugs, and treatments; and determining the length of treatment. In other words, the physician has a key role in determining both the medical need for, and utilization of, many health care services, including those furnished and billed by other providers and suppliers.

Congress has conditioned payment for many Medicare items and services on a certification signed by a physician attesting that the item or service is medically necessary. For example, physicians are routinely required to certify to the medical necessity for any service for which they submit bills to the Medicare program.

Physicians also are involved in attesting to medical necessity when ordering services or supplies that must be billed and provided by an independent supplier or provider. Medicare requires physicians to certify to the medical necessity for many of these items and services through prescriptions, orders, or, in certain specific circumstances, Certificates of Medical Necessity (CMNs). These documentation requirements substantiate that the physician has reviewed the patient's condition and has determined those services or supplies are medically necessary.

Two areas where the documentation of medical necessity by physician certification plays a key role are (i) home health services and (ii) durable medical equipment (DME). Through various OIG audits, we have discovered that physicians sometimes fail to discharge their responsibility to assess their patients' conditions and need for home health care. Similarly, the OIG has found numerous examples of physicians who have ordered DME or signed CMNs for DME without reviewing the medical necessity for the item or even knowing the patient.

Physician Certification for Home Health Services

Medicare will pay a Medicare-certified home health agency for home health care provided under a physician's plan of care to a patient confined to the home. Covered services may include skilled nursing services, home health aide services, physical and occupational therapy and speech language pathology, medical social services, medical supplies (other than drugs and biologicals), and DME.

As a condition for payment, Medicare requires a patient's treating physician to certify initially and rec rtify at least every 62 days (2 months) that:

- the patient is confined to the home;
- the individual needs or needed (i) intermittent skilled nursing care; (ii) speech or physical therapy or speech-language pathology services; or (iii) occupational therapy or a continued need for occupational therapy (payment for occupational therapy will be made only upon an initial certification that includes care under (i) or (ii) or a recertification where the initial certification included care under (i) or (ii));
- a plan of care has been established and periodically reviewed by the physician; and
- the services are (were) furnished while the patient is (was) under the care of a physician.

The physician must order the home health services, either orally or in writing, prior to the services being furnished. The physician certification must be obtained at the time the plan of treatment is established or as soon thereafter as possible. The physician certification must be signed and dated prior to the submission of the claim to Medicare. If a physician has any questions as to the application of these requirements to specific facts, the physician should contact the appropriate Medicare Fiscal Intermediary or Carrier.

Physician Orders and Certificates of Medical Necessity for Durable Medical Equipment, Prosthetics, Orthotics and Supplies for Home Use

DME is equipment that can withstand repeated use, is primarily used for a medical purpose, and is not generally used in the absence of illness or injury. Examples include hospital beds, wheelchairs, and oxygen delivery systems. Medicare will cover medical supplies that are necessary for the effective use of DME, as well as surgical dressings, catheters, and ostomy bags. However, Medicare will only cover DME and supplies that have been ordered or prescribed by a physician. The order or prescription must be personally signed and dated by the patient's treating physician.

DME suppliers that submit bills to Medicare are required to maintain the physician's original written order or prescription in their files. The order or prescription must include:

- the beneficiary's name and full address;
- the physician's signature;
- the date the physician signed the prescription or order;
- a description of the items needed;
- the start date of the order (if appropriate); and
- the diagnosis (if required by Medicare program policies) and a realistic estimate of the total length of time the equipment will be needed (in months or years).

For certain items or supplies, including supplies provided on a periodic basis and drugs, additional information might be required. For supplies provided on a periodic basis, appropriate information on the quantity used, the frequency of change, and the duration of need should be included. If drugs are included in the order, the dosage, frequency of administration, and, if applicable, the duration of infusion and concentration should be included.

Medicare further requires claims for payment for certain kinds of DME to be accompanied by a CMN signed by a treating physician (unless the DME is prescribed as part of a plan of care for home health services). When a CMN is required, the provider or supplier must keep the CMN containing the treating physician's original signature and date on file.

Generally, a CMN has four sections:

- Section A contains general information on the patient, supplier, and physician. **The supplier may complete section A.**
- Section B contains the medical necessity justification for DME. The supplier cannot fill this out. **The physician, a non-physician clinician involved in the care of the patient, or a physician employee, must complete section B.** If the physician did not personally complete section B, the name of the person who did complete section B and his or her title and employer must be specified.
- Section C contains a description of the equipment and its cost. The **supplier completes section C.**
- Section D is the treating physician's attestation and signature, which certifies that the physician has reviewed sections A, B, and C of the CMN and that the information in section B is true, accurate, and complete. **The treating physician must sign section D.** Signature stamps and date stamps are not acceptable.

By signing the CMN, the physician represents that:

- He or she is the patient's treating physician and the information regarding the physician's address and unique physician identification number (UPIN) is correct;
- The entire CMN, including the sections filled out by the supplier, was completed **prior** to the physician's signature; and
- The information in section B relating to medical necessity is true, accurate, and complete to the best of the physician's knowledge.

Improper Physician Certifications Foster Fraud

Unscrupulous suppliers and providers may steer physicians into signing or authorizing improper certifications of medical necessity. In some instances, the certification forms or statements are completed by DME suppliers or home health agencies and presented to the physician, who then signs the forms without verifying the actual need for the items or services. In many cases, the physician may obtain no personal benefit when signing these unverified orders and is only accommodating the supplier or provider. While a physician's signature on a false or misleading certification made through mistake, simple negligence, or inadvertence will not result in personal liability; the physician may unwittingly be facilitating the perpetration of fraud on Medicare by suppliers or providers. When the physician knows the information is false or acts with reckless disregard as to the truth of the statement, such physician risks criminal, civil, and administrative penalties.

Sometimes, a physician may receive compensation in exchange for his or her signature. Compensation can take the form of cash payments, free goods, or any other thing of value. Such cases may trigger additional criminal and civil penalties under the anti-kickback statute.

The following are examples of inappropriate certifications uncovered by the OIG in the course of its investigations of fraud in the provision of home health services and medical equipment and supplies:

- A physician knowingly signs a number of forms provided by a home health agency that falsely represent that skilled nursing services are medically necessary in order to qualify the patient for home health services.
- A physician certifies that a patient is confined to the home and qualifies for home health services, even though the patient tells the physician that her only restrictions are due to arthritis in her hands, and she has no restrictions on her routine activities, such as grocery shopping.
- At the prompting of a DME supplier, physician signs a stack of blank CMNs for transcutaneous electrical nerve stimulators (TENS) units. The CMNs are later completed with false information in support of fraudulent claims for the equipment. The false information purports to show that the physician ordered and certified to the medical necessity for the TENS units for which the supplier has submitted claims.
- A physician signs CMNs for respiratory medical equipment falsely representing that the equipment was medically necessary.
- Physician signs CMNs for wheelchairs and hospital beds without seeing the patients then falsifies his medical charts to indicate that he treated them.
- A physician accepts anywhere from $50 to $400 from a DME supplier for each prescription

Potential Consequences for Unlawful Acts

A physician is not personally liable for erroneous claims due to mistakes, inadvertence, or simple negligence. However, knowingly signing a false or misleading certification or signing with reckless disregard for the truth can lead to serious criminal, civil, and administrative penalties including:

- criminal prosecution;
- fines as high as $10,000 per false claim plus treble damages; or
- administrative sanctions including: exclusion from participation in Federal health care programs, withholding or recovery of payments and loss of license or disciplinary actions by state regulatory agencies.

Physicians may violate these laws when, for example:

- they sign a certification as a "courtesy" to a patient, service provider, or DME supplier when they have not first made a determination of medical necessity;
- they knowingly or recklessly sign a false or misleading certification that causes a false claim to be submitted to a Federal health care program; or
- they receive any financial benefit for signing the certification (including free or reduced rent, patient referrals, supplies, equipment, or free labor).

Even if they do not receive any financial or other benefit from providers or suppliers, physicians may be liable for making false or misleading certifications. Beneficiaries often cannot comprehend the need to scrutinize this information and respond if they feel treatment regimens billed were not representative of actual services provided. In addition busy physician's offices that are already inundated with paperwork really have no means of auditing all treatments provided to their patients in a home care setting. The third element of this program is the added cost sustained by the fiscal intermediaries in implementing and administering a flawed system.

The OIG (Office of Inspector General, Department of Health and Human Services) believes that a home health agency and durable medical equipment providers written policies and procedures should take into consideration the particular statutes, rules, and program instructions that apply to each function of department of the home health agency and durable medical equipment provider. Consequently, we recommend that the individual policies and procedures be coordinated with the appropriate training and educational programs with an emphasis on areas of special concern that have been identified by the OIG through its investigative and audit functions. Some of the special areas of concern include:

- Billing for medically unnecessary services
- Billing for services provided to patients who are not confined to their residence.
- Falsified plans of care
- Untimely and/or forged physician certifications on plans of care

To date there is not a truly effective verification and validation for plan of treatment and certificate of medical necessity verification available that allows a simple and easy means of audit by fiscal intermediaries. If fraud and abuse are to be substantially reduced a truly effective means must be implemented to address these issues. The cost savings to the industry and the improved quality of care would be exponential.

Tracmed.com meets the challenge in the following format as an effective business management tool and answer to compliance issues in a point-by-point fashion:

<u>Billing for medically unnecessary services:</u> HCFA defines billing for medically unnecessary services, involves knowingly seeking reimbursement for a service that is not warranted by patient's current and documented medical condition. Through the use of an electronic treatment eligibility system with encryption technology the patient's physician is able to qualify patient's medical condition and update on a regular basis

<u>Billing for services provided to patients who are not confined to their residence:</u> Through the use of an electronic treatment eligibility system the patient's physician can define homebound status of the patient. This provides an effective documentation system that is far superior to the phone call usually used in current clinical assessment qualifications. The system gives the agency a record of homebound eligibility of patient required by HCFA to meet eligibility criteria for care commencement.

Falsified Plans of Care: Use of an electronic format for submittal of Plans of Care of Certificate of Medical Necessity to physicians with the digital certificate being used by the physician to encrypt and date the care regimen will assure integrity of treatment qualification guidelines.

Untimely and/or forged physician certifications or plans of treatment: The Plan of Care or Certificate for Medical Necessity is electronically submitted to the physician and he enters his digital certificate and encrypts the database. It is automatically presented for billing for the agency or durable medical equipment providers. This provides a time-dated certification and eliminates possibility of backdating documents.

Regulatory Issues

Health Care Fraud & Abuse

The U.S. spends more than $1 billion daily on health care, and government studies extrapolate that up to 10 percent of this spending is tied to fraud and inaccuracy. The prosecution of health care fraud is the Justice Department's second-highest priority, right behind violent crime.

Home health care is the fastest growing expense in the Medicare program, and federal officials believe more than a third of Medicare dollars spent on home care are lost to fraud and abuse.

In a July 1997 report, the Office of Inspector General evaluated a sample of 3,745 services in 250 home health claims in four states and estimated that **40 percent of the services did not meet Medicare reimbursement requirements.** Similarly, the GAO noted significant levels of inappropriate billings in a June 1997 report. A review of 80 high-dollar claims in one state revealed that 43 percent of the claims should have been partially or totally denied.

HIPAA Instituted Changes

The 1996 HIPAA law curbs health care fraud and abuse through increased enforcement of payments. Durable Medical Equipment Providers are reimbursed for Medicare/Medicaid services via fiscal intermediaries – companies that consolidate and manage the payments for the Health Care Financing Administration (HCFA).

HCFA has begun to require fiscal intermediaries to track patterns of billing and utilization by health care providers. The HIPAA bill provides funding to the intermediaries – some $430 million in 1997 alone, and increase by $50 million annually through 2002. Thus, it is guaranteed those investigations; audits and prosecutions of HHAs and DMEs will increase dramatically, beginning almost immediately.

Compliance Requirements

To ensure adherence to HIPAA and the BBA, providers should create an internal compliance program. While not explicitly required by the law, an effective internal compliance program will have a substantial impact in reducing the amount of any fine and penalty under these laws. The program serves as proof of the organization's intent to reduce fraud and abuse.

HCFA Internet Security Policy

The Internet is the fastest growing telecommunications medium in our history. This growth and the easy access it affords have significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among health care providers, HCFA contractors, HCFA components, State agencies acting as HCFA agents, Medicare and Medicaid beneficiaries, and researchers. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The very nature of the Internet communication mechanisms means that security risks cannot be totally eliminated. Up to now, because of these security risks and the need to research security requirements vis-a-vis the Internet, HCFA has prohibited the use of the Internet for the transmission of all HCFA Privacy Act-protected and other sensitive HCFA information by its components and Medicare/Medicaid partners, as well as other entities authorized to use this data.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. Section 5 U.S.C. 552a (e) (10) of the Act is very clear; federal systems must: "...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." One of HCFA's primary responsibilities is to assure the security of the Privacy Act-protected and other sensitive information it collects, produces, and disseminates in the course of conducting its operations. HCFA views this responsibility as a covenant with its beneficiaries, personnel, and health care providers. This responsibility is also assumed by HCFA's contractors, State agencies acting as HCFA agents, other government organizations, as well as any entity that has been authorized access to HCFA information resources as a party to a Data Release Agreement with HCFA.

However, HCFA is also aware that there is a growing demand for use of the Internet for inexpensive transmission of Privacy Act-protected and other sensitive information. HCFA has a responsibility to accommodate this desire as long as it can be assured that proper steps are being taken to maintain an acceptable level of security for the information involved.

This issuance is intended to establish the basic security requirements that must be addressed for use of the Internet to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information.
The term "HCFA Privacy Act-protected Data and other sensitive HCFA information" is used throughout this document. This phrase refers to data that, if disclosed, could result in harm to the agency or individual persons. Examples include:

- All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act; i.e., for which unauthorized disclosure would constitute a "clearly unwarranted invasion of personal privacy" likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.

- Payment information that is used to authorize or make cash payments to individuals or organizations. These data are usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter. As modification of such records could cause an improper payment, these records must be adequately protected.
- Proprietary information that has value in and of it and which must be protected from unauthorized disclosure.
- Computerized correspondence and documents that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.

Policy

This Guide establishes the fundamental rules and systems security requirements for the use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information collected, maintained, and disseminated by HCFA, its contractors, and agents.

It is permissible to use the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information. Detailed guidance is provided below in item 7.

Scope.

This policy covers all systems or processes that use the Internet, or interface with the Internet, to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information, including Virtual Private Network (VPN) and tunneling implementations over the Internet. Non-Internet Medicare/Medicaid data communications processes (e.g., use of private or value added networks) are not changed or affected by the Internet Policy.

This policy covers Internet data transmission only. It does not cover local data-at-rest or local host or network protections. Sensitive data-at-rest must still be protected by all necessary measures, in conformity with the guidelines/rules, which govern the entity's possession of the data. Entities must use due diligence in exercising this responsibility.

Local site networks must also be protected against attack and penetration from the Internet with the use of firewalls and other protections. Such protective measures are outside the scope of this document, but are essential to providing adequate local security for data and the local networks and ADP systems, which support it.

Acceptable Methods

Only authorized parties must access HCFA Privacy Act-protected and/or other sensitive HCFA information sent over the Internet. Technologies that allow users to prove they are who they say they are (authentication or identification) and the organized scrambling of data (encryption) to avoid inappropriate disclosure or modification must be used to insure that data travels safely over the Internet and is only disclosed to authorized parties. Encryption must be at a sufficient level of security to protect against the cipher being readily broken and the data compromised. The length of the key and the quality of the encryption framework and algorithm must be increased over time as new weaknesses are discovered and processing power increases.

User authentication or identification must be coupled with the encryption and data transmission processes to be certain that confidential data is delivered only to authorized parties. There are a number of effective means for authentication or identification, which are sufficiently trustworthy to be used, including both in-band authentication and out-of-band identification methods. Passwords may be sent over the Internet only when encrypted.

Acceptable Approaches to Internet Usage

The method(s) employed by all users of HCFA Privacy Act-protected and/or other sensitive HCFA information must come under one of the approaches to encryption and at least one of the authentication or identification approaches. The use of multiple authentication or identification approaches is also permissible. These approaches are as generic as possible and as open to specific implementations as possible, to provide maximum user flexibility within the allowable limits of security and manageability.

Note the distinction that is made between the processes of "authentication" and "identification". In this Internet Policy, the terms "Authentication" and "Identification" are used in the following sense. They should not be interpreted as terms of art from any other source. Authentication refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet communications data channel itself, generally called an "in-band process." Identification refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path such as the telephone or US mail.

The listed approaches provide encryption and authentication/identification techniques that are acceptable for use in safeguarding HCFA Privacy Act-protected and/or other sensitive HCFA information when it is transmitted over the Internet.

In summary, a complete Internet communications implementation must include *adequate encryption*, employment of *authentication or identification* of communications partners, and a management scheme to incorporate *effective password/key management* systems.

Acceptable Encryption Approaches

Note: As of November 1998, a level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems is recognized by HCFA as minimally acceptable. HCFA reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brute-force exhaustive search).

HARDWARE-BASED ENCRYPTION:

1. Hardware encryptors - While likely to be reserved for the largest traffic volumes to a very limited number of Internet sites, such symmetric password "private" key devices (such as link encryptors) are acceptable.

SOFTWARE-BASED ENCRYPTION:

1. Secure Sockets Layer (SSL) (Sometimes referred to as Transport Layer Security - TLS)
2. At a minimum SSL level have Version 3.0, standard commercial implementations of PKI, or some
3. Variations thereof, implemented in the Secure Sockets Layer are acceptable.
4. S-MIME - Standard commercial implementations of encryption in the e-mail layer are acceptable.
5. In-stream - Encryption implementations in the transport layer, such as pre-agreed passwords, are acceptable.
6. Offline - Encryption/decryption of files at the user sites before entering the data communications process is acceptable. These encrypted files would then be attached to or enveloped (tunneled) within an unencrypted header and/or transmission.

Acceptable Authentication Approaches

AUTHENTICATION (This function is accomplished over the Internet, and is referred to as an "in-band" process.):

1. Formal Certificate Authority-based use of digital certificates is acceptable.
2. Locally managed digital certificates are acceptable, providing the certificates cover all parties to the communication.
3. Self-authentication, as in internal control of symmetric "private" keys, is acceptable.
4. Tokens or "smart cards" are acceptable for authentication. In-band tokens involve overall network control of the token database for all parties.

Acceptable Identification Approaches

IDENTIFICATION (The process of identification takes place outside of the Internet connection and is referred to as an "out-of-band" process.):

1. Telephonic identification of users and/or password exchange is acceptable.
2. Exchange of passwords and identities by U.S. Certified Mail is acceptable.

3. Exchange of passwords and identities by bonded messenger is acceptable.
4. Direct p rsonal contact exchange of passwords and identities between users is acceptable.
5. Tokens or "smart cards" are acceptable for identification. Out-of-band tokens involve local control of the token databases with the local authenticated server vouching for specific local users.

Requirements and Audits

Each organization that uses the Internet to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information will be expected to meet the stated requirements set forth in this document.

All organizations subject to OMB Circular A-130 are required to have a Security Plan. All such organizations must modify their Security Plan to detail the methodologies and protective measures if they decide to use the Internet for transmittal of HCFA Privacy Act-protected and/or other sensitive HCFA information, and to adequately test implemented measures.

HCFA reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this policy. This includes the right to require that any organization utilizing the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive information submit documentation to demonstrate that they meet these requirements.